IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re the Application of: **Michael S. Ripley**

Group Art Unit: **2132**

Application No.: **09/893,177**

Examiner: **Thomas Ho**

Filed: **June 27, 2001**

For: **DISCOURAGING UNAUTHORIZED REDISTRIBUTION OF PROTECTED CONTENT BY CRYPTOGRAPHICALLY BINDING THE CONTENT TO INDIVIDUAL AUTHORIZED RECIPIENTS**

APPEAL BRIEF
IN SUPPORT OF APPELLANT'S APPEAL
TO THE BOARD OF PATENT APPEALS AND INTERFERENCES

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

This brief is in furtherance of the Notice of Appeal, filed in the above-captioned case on February 19, 2009. Applicants (hereafter "Appellants") hereby submit this Brief (37 C.F.R. § 41.37). The fees required under § 41.20(b)(2), and any required petition for extension of time for filing this brief and fees therefore, are dealt with in the accompanying Transmittal of Appeal Brief. Appellants respectfully request consideration of this appeal by the Board of Patent Appeals and Interferences for allowance of the above-captioned patent application. An oral hearing is not desired.

TABLE OF CONTENTS

This brief contains these items under the following headings, and in the order set forth below (37 C.F.R. § 41.37c(1)):

Page 14 of this brief bears the practitioner's signature.

I. REAL PARTY IN INTEREST (37 C.F.R. § 41.37(c)(1)(i))

The real party in interest in this appeal is Intel Corporation of Santa Clara, California, and International Business Machines Corporation of Armonk, New York, by whom the invention is jointly owned.

II. RELATED APPEALS AND INTERFERENCES (37 C F R § 41.37(c)(1)(ii))

With respect to other appeals or interferences that will directly affect, or be affected by, or have a bearing on the Board's decision in this appeal, to the best of Appellant's knowledge, there are no such appeals or interferences.

III. STATUS OF THE CLAIMS (37 C F R § 4137(c)(1)(iii))

The status of the claims in this application are:

A. TOTAL NUMBER OF CLAIMS IN APPLICATION Claims 6, 8, 19, 31-33, are 37-39 are currently pending in the application.

B. STATUS OF ALL THE CLAIMS

1. Claims cancelled: 1-5, 7, 9-18, 20-30, 34-36, and 40-43.
2. Claims withdrawn from consideration but not cancelled: NONE.
3. Claims pending: 6, 8, 19, 31-33, are 37-39.
4. Claims allowed: NONE.
5. Claims rejected: 6, 8, 19, 31-33, are 37-39.

C. CLAIMS ON APPEAL

Claims 6, 8, 19, 31-33, are 37-39 are on appeal.

IV. STATUS OF AMENDMENTS (37 C.F.R. § 41.37(c)(1)(iv))

A response was not submitted in response to the Final Office Action mailed on November 19, 2008. A response was submitted on October 30, 2008, in response to the Office Action mailed on April 30, 2008. The response did not included amendments to the claims, although earlier amendments were submitted and entered. A copy of all claims on appeal is attached hereto as an appendix of claims.

V. SUMMARY OF CLAIMED SUBJECT MATTER (37 C.F.R. * 41.37(c)(1)(v))

There are four independent claims: 6, 19, 31 and 37. Independent claim 6 pertains to a method comprising receiving a request to transfer content to a customer (¶¶0046-47, Figs. 2-3); retrieving from a content source encrypted content corresponding to the requested content, the encrypted content being encrypted by a title key (see, e.g., ¶¶ 0042-44, Fig. 1); obtaining a customer identifier (I.D.) associated with the customer (see, e.g., ¶¶ 0042-44, Fig. 1); binding the requested content to the customer I.D. by using the customer I.D. combined with a media key provided by the content source to encrypt the title key (see, e.g., ¶¶ 0042-44, Fig. 1, ¶¶0046-47, Figs. 2-3); transferring from the content source the encrypted content and the encrypted title key to a non-volatile storage medium (see, e.g., ¶ 0045, Fig. 1) ; and storing the encrypted content and the encrypted title key on the non-volatile storage medium, from which the encrypted content and the encrypted title key may be accessed by the customer (see, e.g., ¶ 0045, Fig. 1).

Claim 19 pertains to memory storage device having stored thereon data representing sequences of instructions, the sequences of instructions which, when executed by a processor, cause the processor to perform the following (see, e.g., ¶ 0013-14): receive a request to transfer content to a customer (see, e.g., ¶¶ 0042-44, Fig. 1, ¶¶0046-47, Figs. 2-3); retrieve from a content source encrypted content corresponding to the requested content, the encrypted content being encrypted by a title key(see, e.g., ¶¶ 0042-44, Fig. 1, ¶¶0046-47, Figs. 2-3); obtain a customer identifier (I.D.) associated with the customer; bind the requested content to the customer I.D. combined with a media key provided by the content source by using the customer I.D. to encrypt the title key (see, e.g., ¶¶ 0042-44, Fig. 1, ¶¶0046-47, Figs. 2-3); transferring from the content

source the encrypted content and the encrypted title key to a non-volatile storage medium; and storing the encrypted content and the encrypted title key on the non-volatile storage medium (see, e.g., ¶ 0045, Fig. 1), from which the encrypted content and the encrypted title key may be accessed by the customer.

Claim 31 pertains to A memory storage device having stored thereon data representing sequences of instructions, the sequences of instructions which, when executed by a processor, cause the processor to perform the following(see, e.g., ¶ 0013-14): access from a non-volatile storage medium content encrypted with a title key accessible by a customer (see, e.g., ¶¶0048-54, Figs. 1, 4, 5) , the non-volatile storage medium additionally storing a customer I.D. associated with the customer requesting the content, a Media Key Block (MKB), and the title key that is encrypted (encrypted title key) with a customer I.D., (see, e.g., ¶¶0048-54, Figs. 1, 4, 5) said processor to access content by: processing the MKB to generate a Media Key by using Device Keys associated with a device for using the content; decrypting the encrypted title key to form the title key by reading a customer I.D., and combining the customer I.D. and the Media Key; and using the title key to decrypt the encrypted content. (See, e.g., ¶¶0048-54, Figs. 1, 4).

Claim 37 pertains to system, comprising: a storage medium; a computer system connected to the storage medium, the computer system (SEE, E.G., ¶¶0013-14) to: access from a storage medium content encrypted with a title key, the storage medium additionally storing a customer I.D. associated with a customer requesting the content, a Media Key Block (MKB), and the title key that is encrypted (encrypted title key) with a customer I.D., (see, e.g., ¶¶0048-54, Figs. 1, 4, 5) the computer to access the encrypted content by: processing the MKB to generate a media key by using Device Keys associated with a device for using the content; decrypting the encrypted title key to form the title key by reading a customer I.D., and combining the customer

I.D. and the Media key; using the title key to decrypt the encrypted content (see, e.g., ¶¶0048-54, Figs. 1, 4, 5).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL (37 C.F.R. § 41.37(c)(1)(vi))

A. Claims 6, 8, and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hirano (U.S. Patent No. 7,145,492) in view of Vanstone (U.S. Patent No. 6,487,661).

B. Claims 31-33 and 37-39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hirano (U.S. Patent No. 7,145,492) in view of Vanstone (U.S. Patent No. 6,487,661) and further in view of Lotspiech (U.S. Patent No. 6,883,097).

VII. ARGUMENT (37 C.F.R. § 41.37(c)(1)(vii))

A. WHETHER CLAIMS 6, 8, AND 19 ARE OBVIOUS OVER HIRANO AND VANSTONE

Claims 1 and 19 are directed to encrypted content, along with a title (content) key used to encrypt the content. However, the title key is provided to a customer in an encrypted form whereby it is encrypted using a customer I.D. *combined with a media key*. Neither Hirano nor Vanstone teach this feature. Hirano does teach content encrypted using an encrypted title key (Hirano calls it an encryption key) encrypted using customer information (see, e.g., Hirano at col. 4, ll. 15-20), but it nowhere teaches encrypting its title (encryption) key using customer information combined with a media key.

In contrast to the Examiner's assertion, however, nowhere does Vanstone teach the use of a key (title or otherwise) encrypted with user information combined with a media key. The Examiner asserts that "Vanstone discloses a key generation method that hashes identification information and a session key to create a shared key (Abstract & Col. 3, lines 8-44), which meets the limitation of combining a media key and the customer I.D. to encrypt the title key."

To begin with, there is no mention in Vanstone of a "shared key." it appears that the examiner is equating this shared key with the title key in Applicant's claims, but there is no reference to a "shared key" in Vanstone. Vanstone's session key is what is used by each party for encrypting/decrypting their messages, i.e., using a common cryptographic function. ("The value of the cryptographic function cannot be compromised or modified without access to the session key." See Abstract and col. 4, ll. 6-25). Therefore, at best, Vanstone's session key is analogous to Applicant's title key, not its media key. Vanstone's session key is not obtained by

decrypting an encrypted session key, let alone, by decrypting an encrypted session key using customer information combined with a media key. It is generated using random integers, generated in real-time by either party during communication between the parties. (See Vanstone at col. 3, ll. 3-40). Therefore, Vanstone's session key is not a media key combined with customer information

Finally, Hirano cannot be combined with Vanstone because Vanstone renders Hirano inoperable for its intended purpose. A primary object of Hirano is to:

> provide a data management method that by encrypting and distributing digital content prevents copyright infringement, and that *prevents authorization information for decrypting the encrypted digital content from being damaged or otherwise lost.*

(See Hirano at col. 2, ll. 7-12) (emphasis added). To do this, it teaches embedding the encrypted key within the content itself (e.g., as a watermark, using extracted sample content) so that the key remains with the downloaded content, i.e., it cannot get separated from it and lost, as could be the case if sent separately from the content. (See Hirano at col. 1, l. 62 to col. 2, l.3). On the other hand, Vanstone teaches an encryption scheme directed to secure, two-way communication between first and second agents (A, B). Vanstone teaches establishing a session key, based on private information from both parties at the time of communications, and using that key for the particular session. (See, e.g., Vanstone Summary). So, if this Hash or key approach is incorporated into Hirano, Hirano's content no longer comes with a self-contained key. This would require the user to request a key every time it wants to play the digital content, not to mention the fact that the key could get separated from the content or get damaged, requiring the user to request another authorization, which goes against express objects of Hirano. Accordingly, the references may not be combined and the rejection should be withdrawn.

B. WHETHER CLAIMS 31-33 AND 37-39 ARE OBVIOUS OVER HIRANO IN VIEW OF VANSTONE AND LOTSPIECH

Independent claims 31 and 37 are also directed to encrypted content techniques including decrypting an encrypted title key using a customer I.D. combined with a Media Key. The Examiner relies on Hirano and Vanstone for teaching these features, as with the above rejected claims. Accordingly, for the same reasons set forth above, Hirano and Vanstone are deficient, and the rejections should be reversed.

CONCLUSION

Based on the foregoing, Appellants request that the Board overturn the rejection of all pending claims and hold that all of the claims of the present application are allowable.

Appellants respectfully petition for an extension of time to respond to the outstanding Office Action pursuant to 37 C.F.R. § 1.136(a) should one be necessary. Please charge our Deposit Account No. 02-2666 to cover the necessary fee under 37 C.F.R. § 1.17 for such an extension.

Respectfully submitted,

Date: May 19, 2009

/Erik Nordstrom, Reg. No. 39,792/

Erik R. Nordstrom
Registration No. 39,792

VIII. CLAIMS APPENDIX (37 C.F.R. § 41.37(c)(1)(viii))

The text of the claims involved in the appeal are:

1.-5. (Cancelled).

6. (Previously Presented) A method comprising:

receiving a request to transfer content to a customer;

retrieving from a content source encrypted content corresponding to the requested content, the encrypted content being encrypted by a title key;

obtaining a customer identifier (I.D.) associated with the customer;

binding the requested content to the customer I.D. by using the customer I.D. combined with a media key provided by the content source to encrypt the title key;

transferring from the content source the encrypted content and the encrypted title key to a non-volatile storage medium; and

storing the encrypted content and the encrypted title key on the non-volatile storage medium, from which the encrypted content and the encrypted title key may be accessed by the customer.

7. (Cancelled).

8. (Original) The method of claim 7, wherein said combining the customer I.D. with a media key comprises using a cryptographic one-way function.

9.-18. (Cancelled).

19. (Previously Presented) A memory storage device having stored thereon data representing sequences of instructions, the sequences of instructions which, when executed by a processor, cause the processor to perform the following:

receive a request to transfer content to a customer;

retrieve from a content source encrypted content corresponding to the requested content, the encrypted content being encrypted by a title key;

obtain a customer identifier (I.D.) associated with the customer;

bind the requested content to the customer I.D. combined with a media key provided by the content source by using the customer I.D. to encrypt the title key;

transferring from the content source the encrypted content and the encrypted title key to a non-volatile storage medium; and

storing the encrypted content and the encrypted title key on the non-volatile storage medium, from which the encrypted content and the encrypted title key may be accessed by the customer.

20.-30. (Cancelled).

31. (Previously Presented) A memory storage device having stored thereon data representing sequences of instructions, the sequences of instructions which, when executed by a processor, cause the processor to perform the following:

access from a non-volatile storage medium content encrypted with a title key accessible by a customer, the non-volatile storage medium additionally storing a customer I.D. associated with the customer requesting the content, a Media Key Block (MKB), and the title key that is encrypted (encrypted title key) with a customer I.D., said processor to access content by:

processing the MKB to generate a Media Key by using Device Keys associated with a device for using the content;

decrypting the encrypted title key to form the title key by reading a customer I.D., and combining the customer I.D. and the Media Key; and

using the title key to decrypt the encrypted content.

32. (Previously Presented) The memory storage device of claim 31, wherein the instructions that cause the processor to combine the customer I.D. and the Media Key comprises instructions that cause the processor to use a crypto-graphic one-way function.

33. (Previously Presented) The memory storage device of claim 31, wherein the content comprises a music title.

34.-36. (Cancelled).

37. (Previously Presented) A system, comprising:

a storage medium;
a computer system connected to the storage medium, the computer system to:

access from a storage medium content encrypted with a title key, the storage medium additionally storing a customer I.D. associated with a customer requesting the content, a Media Key Block (MKB), and the title key that is encrypted (encrypted title key) with a customer I.D., the computer to access the encrypted content by:

processing the MKB to generate a media key by using Device Keys associated with a device for using the content;

decrypting the encrypted title key to form the title key by reading a customer I.D., and combining the customer I.D. and the Media key;

using the title key to decrypt the encrypted content.

38. (Previously Presented) The system of claim 37, wherein the computer system combining the customer I.D. and the Media Key comprises the computer using a cryptographic one-way function.

39. (Previously Presented) The system of claim 37, wherein the content comprises a music title.

40.-43. (Cancelled).

IX. EVIDENCE APPENDIX (37 C.F.R. § 41.37(c)(1)(ix))

To the best of Appellant's knowledge, no evidence has been submitted pursuant to 37 CFR Sections 1.130, 1.131, or 1.132.

X. RELATED PROCEEDINGS APPENDIX (37 C.F.R. § 41.37(c)(1)(x))

(To the best of Appellant's knowledge, there are no related appeals or interferences.)